

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IDEAL AEROSMITH, INC.,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	Civil Action No. 07-1029
	)	
ACUTRONIC USA, INC., <i>et al.</i> ,	)	
	)	
Defendants.	)	

AMBROSE, Chief District Judge

**OPINION AND ORDER**

**Synopsis**

By opinion and order, dated December 13, 2007 [Docket No. 19], I dismissed Plaintiff's claims under the Federal Wiretap and Stored Communications Acts, 18 U.S.C. §§ 2510 *et seq.* and 18 U.S.C. §§ 2701 *et seq.*, and their Pennsylvania state counterparts, 18 Pa. C.S. §§ 5701 *et seq.* and 18 Pa. C.S. §§ 5741 *et seq.*, and the Pennsylvania common law of wrongful procurement/conversion of business information. Defendants now move pursuant to Federal Rule of Civil Procedure 12(c) for judgment on the pleadings with respect to Plaintiff's remaining claims for violation of Pennsylvania's Uniform Trade Secrets Act, unfair competition and civil conspiracy. For the reasons set forth below, I deny Defendants' motion in its entirety.

**I. Legal Standard**

Federal Rule of Civil Procedure 12(c) states: "Motion for Judgment on the Pleadings. After the pleadings are closed - but early enough not to delay trial - a party may move for

judgment on the pleadings.” (West 2008). “Judgment will not be granted unless the movant clearly establishes there are not material issues of fact, and he is entitled to judgment as a matter of law.” Milgrub v. Continental Cas. Co., 2007 WL 625039, at \*3 (W.D. Pa. Feb. 22, 2007) (quoting Sikirica v. Nationwide Ins. Co., 416 F.3d 214, 220 (3d Cir. 2005)). “The Court ‘must view the facts presented in the pleadings and the inferences drawn therefrom in the light most favorable to the nonmoving party.’” Id.

## **II. Background**

Plaintiff’s allegations are discussed in detail in my prior opinion, and therefore, I will only summarize them herein.

In short, Plaintiff Ideal Aerosmith, Inc. (“Ideal”) briefly operated the business of a competitor, Carco Electronics (“Carco”), while Carco was in bankruptcy. In connection with its operation, Ideal hired Carco’s employees and used Carco’s e-mail addresses. Carco was subsequently acquired by Defendant Acutronic USA, Inc. (“Acutronic”). The former Carco employees hired by Ideal did not join Acutronic, but left the Carco premises and remained Ideal employees. These employees were given new Ideal e-mail addresses.

Plaintiff alleges that, despite providing new “Ideal” e-mail addresses, former Carco employees and third parties doing business with Ideal inadvertently continued to send communications using the old Carco e-mail addresses with the Carco domain name. According to Ideal, Acutronic, which now owned the Carco servers, caused the servers to redirect those e-mail messages to an Acutronic server. Acutronic then read the messages, some of which contained Ideal trade secrets and confidential business information, and shared the contents of the messages and/or forwarded the messages to and among certain of its foreign affiliates and

their officers. I refer to these foreign affiliates and their officers as the “Swiss Defendants.”

In my prior opinion, I held, in part, that Acutronic, as the owner of the Carco server to which the e-mails inadvertently were sent, had a right under the Federal Stored Communications Act to access those e-mails. In dismissing Plaintiff’s wrongful procurement and Wiretap Claims, I further held that Plaintiff had not engaged in any wrongdoing in accessing and reading those e-mails. The issue before the Court now comes down to whether Defendants’ alleged use and disclosure of the contents of the e-mails states a valid claim under Pennsylvania law.

### **III. Defendants’ Motion for Judgment On The Pleadings**

#### **A. Federal Preemption, Generally**

Defendants argue that the remaining claims, for violation of Pennsylvania’s Uniform Trade Secrets Act, unfair competition and civil conspiracy, are preempted by the federal Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.* (the “SCA”). According to Defendants, the SCA was meant to provide a “comprehensive statutory scheme addressed to electronic storage,” (Def. Br. at 17), and the SCA “makes it perfectly lawful for an electronic communications service provider to access, use and disclose anything landing on its servers.” (Def. Br. at 6.)

“Under the Supremacy Clause, when state law conflicts or is incompatible with federal law, the federal law preempts the state law.” Surrick v. Killion, 449 F.3d 520, 531 (3d Cir. 2006). As the Third Circuit recently explained: “Preemption is not a doctrine which lends itself to a black-letter rule. One size does not fit all. The decision must be based on the circumstances presented in the particular situation.” Colacicco v. Apotex Inc., 2008 WL 927848, at \*1 (3d Cir. Apr. 8, 2008). “Preemption generally occurs in three ways: (1) where Congress has expressly preempted state law; (2) where Congress has legislated so comprehensively that federal law

occupies an entire field of regulation and leaves no room for state law; or (3) where federal law conflicts with state law.” Id. at \*5. Defendants argue that each of these bases support their argument that the SCA preempts Plaintiff’s state law claims.

### **B. The Scope of The SCA**

In order to determine whether preemption applies, it is first necessary to understand the terms and scope of the SCA. While I discussed the SCA to some extent in my prior opinion, I feel that additional clarification is necessary in this context.

Section 2701 of the SCA, entitled “Unlawful access to stored communications,” provides:

(a) Offense.— Except as provided in subsection (c) of this section whoever - (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.” 18 U.S.C. 2701(a). Subsection (c) exempts from liability for the conduct described in subsection (a) “those persons or entities providing a wire or electronic communication service;” and “a user of that service with respect to a communication of or intended for that user.” 18 U.S.C. 2701(c). Thus, as I previously held, section 2701 prohibits only the unauthorized access to stored communications.

By contrast, sections 2702 and 2703 address the disclosure of the contents of stored communications in two narrow contexts. Section 2702, entitled “Voluntary disclosure of customer communications or records,” provides, in relevant part, that “(1) a person or entity providing an electronic communication service *to the public* shall not knowingly divulge to any

person or entity the contents of a communication while in electronic storage by that service; and (2) a person or entity providing remote computing service *to the public* shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service. . . .” (Emphasis added.) Subsection (b) sets forth the limited circumstances in which a person or entity described in subpart (a) may disclose communications, such as with the sender or recipient’s permission, or to a law enforcement agency where the contents appear to pertain to the commission of a crime. 18 U.S.C. 2702(b). Section 2703 of the SCA addresses the circumstances under which *a governmental entity* can require a provider of electronic communication service to disclose the contents of the communications pursuant to a warrant or court order. 18 U.S.C. 2703(a)-(b). Finally, section 2707 provides a civil cause of action for any person or entity “aggrieved by any violation of this chapter.”

The legislative history of the SCA supports the limited nature of its provisions. As I previously explained, the “general purpose of the Stored Communications Act was to ‘create a cause of action against computer hackers (e.g. electronic trespassers).’” [Docket No. 19, at 12] (quoting International Ass’n of Machinists and Aerospace Workers v. Werner-Masuda, 390 F. Supp.2d 479, 495 (D. Md. 2005)). In further discussing the disclosure provisions of sections 2702 of the SCA (and 2511 of the Wiretap Act), it states that “[n]either provision, however, nor any other provision in the Act, is intended to affect any other provision of federal law that prohibits the disclosure of information on the basis of the content of the information, such as the Fair Credit Reporting Act.” S. Rep. 99-541, at 37.

I now turn to Defendants’ preemption arguments.

### **1. Express Preemption**

Express preemption applies where the statute at issue explicitly provides that its enactment pre-empts state law. Fasano v. Federal Reserve Bank of N.Y., 457 F.3d 274, 280 (3d Cir. 2006), cert. denied, 127 S.Ct. 977 (2007). Section 2708 of the SCA states that “[t]he remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.” 18 U.S.C. §2708. Defendants interpret this provision as an explicit mandate of preemption for all claims that “touch upon the subject matter that is addressed” in the SCA. (Def. Br. at 8.)

There is little case law interpreting whether or not section 2708 expresses a Congressional intent that the SCA preempt state law claims, and much of it is conflicting. As both parties have recognized, the Senate Report on the bill does not address the language of 2708, but does discuss identical language in section 2518 of the Wiretap Act, explaining that “[t]he purpose of this provision is to underscore that, as a result of discussions with the Justice Department, the Electronic Communications Privacy Act does not apply the statutory exclusionary rule contained in title III of the Omnibus Crime Control and Safe Streets Act of 1968 to the interception of electronic communications.” S. Rep. 99-541, at 23. The only case in this Circuit which has addressed the issue has held that the SCA does *not* expressly preempt state law, explaining that “the purpose of [2708] is not to expressly preempt state law, but rather to establish that the exclusionary rule is not a remedy provided for by the Act.” Bansal v. Russ, 513 F. Supp.2d 264, 282 (E.D. Pa. 2007) (denying motion to dismiss claims under the SCA and Pennsylvania’s Wiretapping and Electronic Surveillance Control Act); see also, In re Nat’l Sec. Agency Telecom. Records Litig., 483 F. Supp.2d 934, 939 (N.D. Ca. 2007) (interpreting 2708 to preclude suppression as a remedy and holding that “the SCA does not completely preempt suits

under state law”).

Defendants rely on Quon v. Arch Wireless Operating Co., Inc., 445 F. Supp.2d 1116 (C.D. Ca. 2006), to support their argument that 2708 contains an express preemption of state law claims. I disagree with the applicability of Quon to the allegations herein. There were two sets of defendants in Quon, the City of Ontario and its police department (the “governmental defendants”), and Arch Wireless, from which the governmental defendants contracted for text-messaging pager service. The district court held that Arch Wireless was exempt from liability for disclosure because, as a “entity providing an electronic communication service to the public” or an “entity providing remote computing service to the public” under 2702(a), it met the exception for disclosure at the request of the subscriber set forth in 2703(b)(3). The court held that “in enacting the SCA, Congress left no room for supplementary state regulation for conduct covered by the statute.” 445 F. Supp.2d at 1138. Accordingly, because Arch Wireless’ disclosure was expressly condoned by section 2703, the court held that section 2708 preempts a state law which would render Arch Wireless liable for the identical conduct. Id. (granting summary judgment dismissing SCA and state invasion of privacy and constitutional claims against Arch Wireless)<sup>1</sup>; see also, Muskovich v. Crowell, 1995 WL 905403, at \*1 (S.D. Iowa Mar. 21, 1995) (“In section 2708, Congress unequivocally expressed an intent to ‘occupy the field’ and provide the exclusive remedies for conduct regulated by ECPA.”)

While I tend to agree with Defendants that the language of 2708 seems facially to contain an express preemption, at least with respect to remedies, I need not decide that issue, because it is

---

<sup>1</sup>The court in Quon also granted summary judgment dismissing the SCA claims against the governmental defendants for the same reasons that we dismissed those claims herein, i.e. that the governmental defendants’ access to the communications was condoned by section 2701(c).

inapplicable to the allegations herein. Indeed, the court's reasoning in Quon underlies the flaw in Defendants' reliance on any form of preemption. As discussed in detail above, the SCA regulates the disclosure of the contents of stored communications in two situations: (1) under 2702, where the party provides an electronic communication service to the public or a remote computing service to the public; and (2) under 2703, to a governmental entity which obtains a court order, warrant or administrative subpoena in connection with a criminal investigation. The court in Quon found preemption applied because the conduct of Arch Wireless, an entity which provided electronic communication service to the public, was expressly addressed by the SCA. Here, however, Acutronic undisputedly did *not* provide an electronic communication or remote computing service to the public, nor did it disclose the contents of the e-mails to a governmental entity in connection with a criminal investigation. Thus, Acutronic's conduct is not addressed by the SCA's disclosure provisions. Accordingly, the so-called "preemption clause" by its terms does not apply herein.

I must note that Defendants' characterization of my prior opinion is a gross overstatement. I certainly did not hold that "Acutronic has federal immunity ('an unfettered right') to engage in this conduct - i.e., to access, disclose and use the emails." (Def. Br. at 11). Rather, in dismissing the claims under the SCA and its Pennsylvania counterpart, I held that Acutronic had the right under the SCA to access the e-mails, and that section 2701 of the SCA did not prohibit the use or disclosure of that information. [Docket No. 19, at 14.] Since Acutronic had the right to access the e-mails, and the use and disclosure of them was not prohibited by the SCA, then Acutronic could not be liable under the SCA for its conduct. I certainly did not hold that the SCA provided any immunity for the use and disclosure of the



contents of the e-mails.<sup>2</sup>

## **2. Field Preemption**

Since Acutronic's conduct is not directly addressed by the SCA, the question then becomes whether the Pennsylvania state laws at issue "regulate[] conduct in a field that Congress intended the Federal Government to occupy exclusively." Fasano, 457 F.3d at 280. While Defendants discuss the congressional intent behind the original Wiretap Act of 1968, they do not discuss the intent of Congress in amending the Wiretap Act to include the Stored Communications Act at issue herein. I have looked at the limited evidence on this issue, (see Part III(B) above) and find that it does not support Defendants' claim of field preemption. Neither the language of the SCA itself nor the Congressional record demonstrate an intent to regulate the entire field governing the disclosure of stored communications. Accordingly, I hold that Plaintiff's state law claims are not subject to field preemption.

## **3. Conflict Preemption**

Conflict preemption analysis "is designed to determine the propriety of preemption where Congress has not explicitly stated its intent." Colacicco, 2008 WL 927848, at \*8. "A conflict between state and federal law 'arises when compliance with both federal and state regulations is a physical impossibility or when state law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress.'" Id. at \*9; see

---

<sup>2</sup>My holding is consistent with the Court's holding in Quon that "the governmental defendants do not fall within the statutory prohibitions contained in section 2702(a), that section 2703 has no application to the facts of this case, and therefore, those defendants are not liable *under the Act* for any disclosure of the contents of the text messages received or transmitted from [plaintiff's] pager." 445 F. Supp.2d at 1129-30 (emphasis added). Notably, the court in Quon did not hold that the SCA preempted any state law claims relating to the governmental defendants' disclosure of the contents of the communications.

also, Fasano v. Federal Reserve Bank of N.Y., 457 F.3d at 283 (“Conflict preemption arises in the absence of specific preemption language, where an individual is unable to follow both federal and state law simultaneously, or where the state law would frustrate the federal scheme.”)

Defendants’ argument for conflict preemption fails for the same reason I have found no express or field preemption - that the conduct at issue is simply not covered by the SCA. Defendants are asking this Court to infer from the right granted by the SCA to a private electronic communication service provider to monitor its system a concomitant right to use and disclose with impunity the contents of those communications. There is simply no legal support for this position. The SCA addresses the disclosure of content only in very limited circumstances, in the context of providers of communication service to the public and where required by a governmental entity in accordance with certain defined procedures. If Congress had intended for the SCA to create a blanket right to disclosure, it could have done so without bothering to carve out these narrow exceptions. Its failure to do so implies the opposite of what Defendants argue, i.e. that Congress never intended to grant wholesale immunity to private service providers to use and disclose without authorization the contents of communications on their system. See Hill v. Park, 2004 WL 180044, at \*3 (E.D. Pa. Jan. 27, 2004) (“The canon of *expressio unius est exclusio alterius* means that explicit mention of one thing in a statute implies a congressional intent to exclude similar things that were not specifically mentioned.”)

The gist of Plaintiff’s misappropriation of trade secrets claim is less the access to the communication, than Defendants’ recognition of its contents as trade secrets and their alleged unauthorized use and disclosure of those trade secrets, including to unfairly compete with Plaintiff. Since the SCA does not address the unauthorized disclosure and use of the contents of

stored communications by private service providers, it is not in conflict with the state laws at issue herein.

Based on the foregoing, I deny Defendants' motion for judgment on the pleadings dismissing Count 3 of the Complaint.

### **C. Unfair Competition and Conspiracy**

Defendants argue that the Pennsylvania Uniform Trade Secrets Act, 12 Pa.C.S.A. 5301 *et seq.* ("PUTSA"), preempts Plaintiff's state law claims for unfair competition and civil conspiracy. Section 5308 of PUTSA provides: "Except as provided in subsection (b), this chapter displaces conflicting tort, restitutionary and other law of this Commonwealth providing civil remedies for misappropriation of trade secret." 12 Pa.C.S.A. 5308. Subsection (b) provides, in relevant part: "This chapter does not affect. . . (2) other civil remedies that are not based upon misappropriation of trade secret." *Id.*

Where there has been no determination that the information at issue constitutes a trade secret within the purview of PUTSA, courts have been reluctant to dismiss related state law claims. *See Weiss v. Fiber Optic Designs, Inc.*, 2007 WL 3342605, at \*1 (E.D. Pa. Nov. 9, 2007) (denying motion to dismiss unfair competition claim where the plaintiff argued that the claim was premised on wrongdoing distinct from the misappropriation claim); *Cenveo Corp. v. Slater*, 2007 WL 527720, at \*3 (E.D. Pa. Feb. 12, 2007) (refusing to dismiss conversion claim prior to determination of whether the information at issue constituted a trade secret). The case cited by Defendants is not to the contrary. *See Firsttrust Bank v. Didio*, 2005 WL 2001105, at \*1 (Pa. Com. Pl. July 29, 2005) (dismissing only those claims based solely on defendants' theft of the trade secrets).

Defendants have not cited any authority to the Court that Plaintiff as a matter of law cannot prove a claim for unfair competition distinct from its claim under PUTSA. It may well be, in the end, that Plaintiff's unfair competition claim is preempted. But this is not the stage of the litigation to do so. Similarly, Defendants have failed to cite to any case law dismissing conspiracy claims in the face of valid claims under PUTSA or the common law of unfair competition. Accordingly, I deny Defendants' motion for judgment on the pleadings dismissing Counts 7 and 8 of the Complaint.

### **CONCLUSION**

For the reasons set forth above, I deny Defendants' motion for judgment on the pleadings in its entirety.

### **ORDER OF COURT**

AND NOW, this 23rd day of April, 2008, after careful consideration, and for the reasons set forth in the accompanying Opinion, Defendants' motion for judgment on the pleadings (Docket No. [46]) is denied in its entirety.

BY THE COURT:

/s/ Donetta W. Ambrose

Donetta W. Ambrose,  
Chief U.S. District Judge